





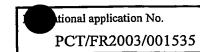
PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference BdR/BR 60677	FUR FUR I DEN ACTION Declinings Eventingtion Report (Form PCI/IPEA/410)			
International application No. PCT/FR2003/001535	International filing date 21 mai 2003 (2		Priority date (day/month/year) 05 juin 2002 (05.06.2002)	
International Patent Classification (IPC) or n H04L 9/32	ational classification and	IPC		
Applicant FRANCE TELECOM				
 This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36. 				
2. This REPORT consists of a total of	5 sheets, i	including this cover	sheet.	
This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).				
These annexes consist of a to	otal ofs	heets.		
3. This report contains indications rela	ating to the following iten	ns:		
I Basis of the report				
II Priority				
III Non-establishment	of opinion with regard to	novelty, inventive s	tep and industrial applicability	
IV Lack of unity of in	I calc of unity of invention			
Peasoned statemen	V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement			
VI Certain documents	VI Certain documents cited			
VII Certain defects in t	VII Certain defects in the international application			
VIII Certain observation	VIII Certain observations on the international application			
Date of submission of the demand		Date of completion	of this report	
19 décembre 2003 (19.	12.2003)	10 N	lovember 2004 (10.11.2004)	
Name and mailing address of the IPEA/EF		Authorized officer		
Facsimile No.		Telephone No.		





I. I	Basis o	f the re	port	
1.		-	the elements of the international application:*	
		the inter	mational application as originally filed	
	\boxtimes	the desc	cription:	
		pages .	1-13	, as originally filed
		pages .	Clad with the letter of	, filed with the demand
		pages	, filed with the letter of	
	\boxtimes	the clain	ms:	
		pages	1-14	, as originally filed
		pages	, as amended (together with an	, filed with the demand
		pages	, filed with the letter of	,
	\bowtie	the drav	-	, as originally filed
		pages	1/3-3/3	
		pages pages	, filed with the letter of	
	—			
	Ш ü	-	ence listing part of the description:	as originally filed
		pages pages		, filed with the demand
		pages	, filed with the letter of	
2.	the in	nternation e elemen the lan the lan	Inguage of a translation furnished for the purposes of international search (under Rule 23.1) aguage of publication of the international application (under Rule 48.3(b)). Inguage of the translation furnished for the purposes of international preliminary examinates.	which is: (b)).
3.	With prelii	regard minary e	to any nucleotide and/or amino acid sequence disclosed in the international a examination was carried out on the basis of the sequence listing:	pplication, the international
		contai	ned in the international application in written form.	
			ogether with the international application in computer readable form.	
ļ			hed subsequently to this Authority in written form.	
	Ц		hed subsequently to this Authority in computer readable form.	and the disclosure in the
		interna	statement that the subsequently furnished written sequence listing does not go be ational application as filed has been furnished.	
			tatement that the information recorded in computer readable form is identical to the furnished.	written sequence usting has
4.	П	The a	mendments have resulted in the cancellation of:	
		\Box	the description, pages	
			the claims, Nos.	
			the drawings, sheets/fig	
5.	. 🔲	This re	eport has been established as if (some of) the amendments had not been made, since the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**	y have been considered to go
	in th	is repo	t sheets which have been furnished to the receiving Office in response to an invitation un rt as "originally filed" and are not annexed to this report since they do not conta	nder Article 14 are referred to ain amendments (Rule 70.16
	ana i Any i	70.17). replacen	ment sheet containing such amendments must be referred to under item 1 and annexed to t	this report.



INTERNATIONAL PRE INARY EXAMINATION REPORT

ĺ	International	application No.
	P FR	03/01535

/ .	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability;
	citations and explanations supporting such statement

Statement			
Novelty (N)	Claims	1-14	YES
	Claims		NO
Inventive step (IS)	Claims	3-7, 9	YES
mromaro susp (12)	Claims	1, 2, 8, 10-14	NO
Industrial applicability (IA)	Claims	1-14	YES
••	Claims		NO

Citations and explanations

Reference is made to the following documents:

D1: US-B-6 215 872 B1 (VAN OORSCHOT PAUL C) 10 April 2001 (2001-04-10)

D2: EP-A-0 856 821 (NIPPON TELEGRAPH & TELEPHONE) 5 August 1998 (1998-08-05)

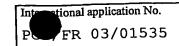
The present application fails to comply with the requirements of PCT Article 33(1) since the subject matter of claims 1, 2, 8 and 11 to 14 does not involve an inventive step (PCT Article 33(3)).

Document D1, which is considered to be the prior art closest to the subject matter of claim 1, describes (see column 4, lines 11-42; column 5, lines 2-5; column 8, line 60 to column 9, line 12; the reference signs between parentheses apply to this document):

An electronic signature verification method involving a user having a data processing system, wherein the user receives electronic signature verification requests from the data processing system and processes said requests, an electronic signature is generated by means of a private key known only to a signatory entity and combined with a public key, the method includes a storage step carried out

INTERNATIONAL PREMINARY EXAMINATION REPORT

1



in a certificate table (trusted public key list 36) containing a compressed form of at least one public key, and an electronic signature verification process comprising the steps of: receiving the electronic signature to be verified and a public key in a pair of keys including a private key previously used to generate the electronic signature to be verified, computing a compressed form of the received public key, searching the certificate table (36) for the computed compressed form of the public key, and decrypting the electronic signature by means of the received public key when the computed compressed form of the public key is found in the certificate table.

It follows that the subject matter of claim 1 differs from this known method only in that the method involves the use of a microcircuit connectable to a data processing system, and in that the certificate table is stored in a microcircuit memory.

The problem that the present invention, as defined in claim 1, is intended to solve can thus be considered to be the practical implementation of the known method. However, storing certificates and public keys in a smart card memory is known (see D2, figure 4B, column 5, line 57 to column 6, line 29). A person skilled in the art would certainly use such a card to carry out the method according to D1, and would thus arrive at the subject matter of claim 1 without exercising inventive skill.

The same argument is applicable mutatis mutandis to the subject matter of the corresponding independent claims 13 and 14, which thus lack an inventive step.

Dependent claim 2 does not contain any additional feature

which, in combination with claim 1, might define subject matter that complies with the requirements of PCT Article 33(3), for the following reasons:

The additional steps mentioned are equivalent to conventional received certificate verification; a person skilled in the art would carry out this procedure before inserting a public key or a compressed form thereof in order to be sure of the authenticity of the received certificate, and would thus arrive at the subject matter of claim 2 without exercising inventive skill.

Dependent claims 8, 10, 11 and 12 do not contain any features which, when combined with the features of any one of the claims to which they refer, might define subject matter that complies with the requirements of inventive step of the PCT (see documents D1 and D2 and the corresponding passages cited in the search report).

The combination of features in claim 3 is not found in or obvious from the prior art, for the following reasons: no prior art document discloses inserting a pointer to the compressed form of the public key of the certifying entity that issued a certificate, thereby defining a certification tree stored in a microcircuit memory. The combination of features in claim 9 likewise is not found in or obvious from the prior art.

Therefore, claims 3 and 9 comply with the requirements of PCT Article 33(2) and (3).

Assuming that claims 4 to 6 are dependent on claim 3, they too comply, as such, with the requirements of novelty and inventive step of the PCT.

Contrary to the requirement of PCT Rule 5.1(a)(ii), the relevant prior art disclosed in documents D1 and D2 has

not been indicated in the description, nor have these documents been cited.

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:
☐ BLACK BORDERS
LIMAGE CUT OFF AT TOP, BOTTOM OR SIDES
☐ FADED TEXT OR DRAWING
☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
☐ SKEWED/SLANTED IMAGES
☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
☐ GRAY SCALE DOCUMENTS
☐ LINES OR MARKS ON ORIGINAL DOCUMENT
☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
<u> </u>

IMAGES ARE BEST AVAILABLE COPY.

☐ OTHER:

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.